31/0027/rev.2

NRC security: YOU ARE THE KEY

NEWARK PUBLIC LIBRARY

AUG 1 9 1986

U. S. GOVT. PUBS.
DEPOSITORY 376

UNITED STATES
NUCLEAR REGULATORY
COMMISSION

Y3.N88:

THIS PUBLICATION CONTAINS NO CLASSIFIED OR
SENSITIVE UNCLASSIFIED INFORMATION.

PREFACE

This booklet has been prepared to provide you general information regarding Nuclear Regulatory Commission (NRC) security policies and procedures and to provide an appreciation for their necessity.

In addition to the information in this booklet and in NRC Management Directive 2000, which provides detailed guidance on the NRC Security Program, the staff members of the Division of Security (SEC) are always available to assist you on any NRC security-related matter. However, YOU ARE THE KEY TO NRC SECURITY.

Raymond J. Brady

Raymond J. Brady, Director
Division of Security
Office of Administration

INTRODUCTION

The Nuclear Regulatory Commission (NRC) is the Federal agency responsible for licensing and regulating the civilian use of nuclear materials and facilities in a manner consistent with health and safety, environmental quality, national security and antitrust laws. These important responsibilities result in NRC employees handling significant quantities of classified and sensitive unclassified information. Therefore, each NRC employee -- new and old -- plays a key role in making certain that security policies and procedures are followed to protect classified and sensitive unclassified information, government and personal property, and, from a larger perspective, our nation's security and the safety of the public.

READEX FICHE best copy available

YOU ARE THE KEY TO NRC SECURITY

NRC SECURITY PROGRAM

Sensitive Unclassified Information

Most NRC offices handle more sensitive unclassified information than classified information. The types of sensitive unclassified information are: Official Use Only (OUO); Limited Official Use (LOU); Proprietary; and Safeguards Information.

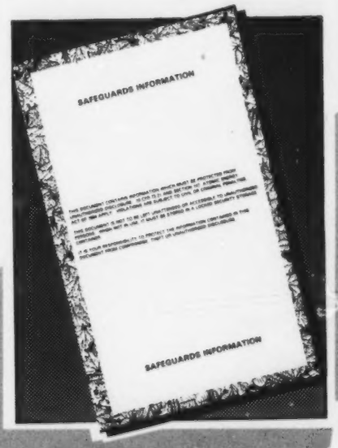
Official Use Only or OUO information is handled by most NRC offices. OUO information includes personal and privacy data such as personnel and payroll records and performance appraisals. Other OUO information may include staff policy positions or decisions being formulated prior to their public release.

Limited Official Use information, often referred to as LOU, designates certain information received from the Department of State.

Proprietary information is someone else's "property" that has been entrusted to NRC. Traditionally it has included trade secrets and commercial or financial data. Additionally, information regarding the protection of special nuclear material and information received in confidence from a foreign source has been deemed to require the same protection afforded proprietary information.

It is important to realize that for Privacy Act (OUO) and Proprietary information, you can be held personally liable for damages associated with an unauthorized disclosure.

Safeguards Information may include an applicant's or licensee's detailed physical security plan for the protection of special nuclear material or information concerning certain plant equipment vital to the safety of production. Civil and criminal penalties stated in the Atomic Energy Act of 1954, as amended, can be levied for the unauthorized disclosure of Safeguards Information.



Access to Sensitive Unclassified Information

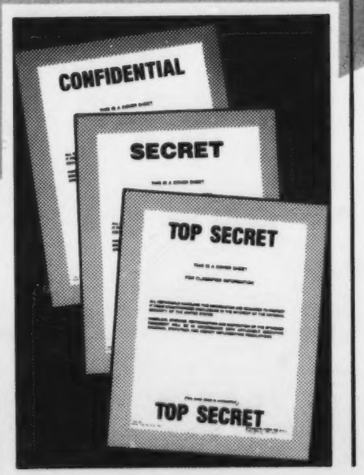
Access to sensitive unclassified information does not require an NRC security clearance (access authorization). However, before sharing this information with anyone else, even a co-worker, be certain that the individual requires the information to perform official, contractual or licensee duties. That is, an official need-to-know must exist for access. Need-to-know must be assured, not assumed.

Since a security clearance is not required for access to sensitive unclassified information, employees who begin work prior to the completion of their security clearance processing (a procedure permitted by Section 145b of the Atomic Energy Act of 1954, as amended) may have access to sensitive unclassified information if they have an official need-to-know.

Classified Information

Even though you may not routinely handle classified information or material in your work, you still should be familiar with the categories and levels of classified information and the proper handling procedures.

NRC handles two basic categories of classified information: National Security Information (NSI), and Restricted Data (RD). NSI is defined and protected according to the provisions of the President's Executive Order and the Information Security Oversight Office Directives. RD is defined and protected according to the provisions of the Atomic Energy Act of 1954, as amended. Within each of these categories of classified information, NSI and RD, there are three levels of classification according to the sensitivity of the information. In declining order of sensitivity, they are TOP SECRET, SECRET, and CONFIDENTIAL. Unauthorized disclosure at each level could cause a corresponding level of damage to the national security. The unauthorized disclosure of TOP SECRET information could be expected to cause exceptionally grave damage to the national security. Disclosure of SECRET information could cause serious damage, while disclosure of CONFIDENTIAL information could damage the national security.



Only an authorized classifier may make classification, downgrading, and declassification determinations. Draft and final documents that may contain classified information should be reviewed by an authorized classifier. If you do not have an authorized classifier available, or you believe a document is improperly classified, contact SEC.

Access to Classified Information

The same principle of need-to-know applies for access to classified information, but there is the added requirement of having the appropriate level of security clearance. New employees who begin work without a security clearance are to have NO ACCESS to any level of classified information until their security clearance has been granted. These individuals should wear their NO ACCESS badge in clear view to alert others that their security clearance is still pending.

You should be aware that foreign nationals, including those who may visit or work for the NRC, are not permitted access to classified information or material and must be restricted to physical areas approved in their security plan. Those foreign nationals without an approved security plan must be escorted while at work.

Personnel Security Clearances

For NRC employees SEC grants two types of security clearances. After an appropriate background investigation is conducted and any eligibility concerns are resolved, an "L" or a "Q" clearance is granted.

The type of security clearance you receive is determined by the sensitivity of the position you occupy, and the level of access to classified information required in the performance of your official duties. A "Q" security clearance allows access up to Top Secret National Security Information and Restricted Data, whereas the "L" security clearance allows access to the Confidential level of Restricted Data and the Secret and Confidential levels of National Security Information.

There are also reporting requirements associated with your security clearance. NRC Form 176, "Security Acknowledgment," requires you to advise SEC of all arrests, charges or detentions by Federal, State or other law enforcement authorities, excluding traffic violations with a fine of $100.00 or less. Also report marriage subsequent to your last investigation; and any other event or circumstance which could have a bearing on the continuation of your security clearance.

Although some employees may never handle classified information, all NRC employees, after having been granted their security clearance, complete the Standard Form 189, "Classified Information Nondisclosure Agreement." Through this agreement, the employee agrees not to disclose classified information to any person who does not have an appropriate security clearance or does not have a demonstrated official need-to-know.

Protection of Information

NRC Management Directive 2000, "NRC Security Program," provides guidance on the storage and handling of sensitive unclassified and classified information. This guidance includes: use of appropriate cover sheets; accurate security markings; proper transmission; adequate storage when information is unattended; reproduction only as necessary: proper destruction; and use of discretion in choosing when and where to discuss such information. Remember that no matter what form the sensitive unclassified or classified information is in, whether a final document, on a diskette, a draft or on a typewriter/printer ribbon used for the document, the information needs to be protected according to its level of sensitivity.

More specifically, classified information must be stored when unattended in an approved security container or vault-like room. Remember also, that

YOU ARE THE KEY TO NRC SECURITY

an open container or vault-like room requires observation by an individual with the appropriate security clearance for the level of classified information in the container or vault-like room; that prior to transmitting classified information, assure that the recipient has such storage available; and that lock combinations must be memorized and changed at least annually. Failure to comply with proper handling and protection requirements may result in the disclosure of classified information for which there are serious sanctions or, at a minimum, issuance of a security infraction to the individual responsible.

The increasing use of computers, ADP and word processing equipment makes us more productive and our work easier. However, the proper protection of information processed by these systems and equipment is essential. ONLY under special circumstances, and with the written authorization of SEC, may classified information be processed or telecommunicated on automated systems.

Sensitive unclassified information may be processed on the IBM 5520 shared logic word processing system, stand-alone equipment (e.g., Displaywriter), personal computers, and certain other ADP systems if administrative access and security control

procedures are strictly followed. In general these procedures include: the use of system security features (e.g., passwords, user I.D.); the proper marking, protection or destruction of printer ribbons, output and diskettes specifically established for sensitive unclassified information; and never leaving a system unattended when processing sensitive unclassified information.

Another communications medium you should use with discretion is the telephone. Telephone systems used for computer hookups, for transmittal of information via facsimile, and for normal business use are vulnerable to interception. The more you use the telephone, especially for long distance calls, the more susceptible you are to undetected eavesdropping by anyone wishing to exploit your sensitive unclassified conversations.

With the increased use of terrestrial microwave relays and satellites for transmission of telephone signals and the availability of sophisticated monitoring equipment, signals can be intercepted with no physical connection to the telephone or telephone line. Detecting such intercepts is nearly impossible. Because the methods for remotely intercepting regular telephone transmissions are well known to intelligence, security and communications specialists throughout the world, classified and sensitive unclassified information must only be telecommunicated in a protected manner. Specifically, classified information must be communicated over NRC's Secure Telephone Units or by secure teletype/facsimile equipment. In addition to the above methods for communicating classified information, sensitive unclassified information may be telecommunicated in an encrypted mode between NRC Headquarters and Regional Offices on the IBM 5520 shared logic word processing system. Secure voice, facsimile and teletype facilities are available within NRC.

Travel/Meetings

Travel and meeting arrangements should often involve SEC in order to assure the protection of classified or sensitive unclassified information. Certification of clearance and need-to-know must be provided for outgoing and incoming visits with employees of other Government agencies, national laboratories and some contractors when the visit involves classified information. This is accomplished by the completion and processing of an NRC Form 277, "Request for Visit or Access Approval." Another important reason for coordinating travel arrangements with SEC is for your personal protection. If you travel abroad, particularly to Communist-controlled countries, SEC would like to advise you of valuable precautions that should be taken when travelling.

Clandestine intelligence activities do exist, as accounts in various publications and news articles have portrayed. There is a conscious, determined effort by foreign governments

and others to obtain classified, proprietary, economic, technical, political and other sensitive information. You should use prudent judgment at all times in deciding when, where, and with whom you discuss classified or sensitive unclassified information. Additionally, you should report any attempt to use you to obtain illegal or unauthorized access to classified or otherwise sensitive information or if you are concerned that you may be the target of an attempted exploitation by a foreign entity.

Physical Security

Photo clearance badges, key cards, keys, guards and other forms of access control are used for access to

NRC-controlled areas. When you admit individuals not known to you, the effectiveness of the physical security measures are reduced. Do not admit anyone whom you do not know, are not expecting or is not otherwise authorized. Also, promptly notify SEC of any suspected theft or suspicious incidents. Physical security measures are used to protect you, personal possessions, Government property, and facilities where sensitive unclassified and classified information are located. However, each individual employee is a key to ensuring maximum security.

SUMMARY

This booklet has provided you general guidance on: the types of information NRC needs to protect; the security clearances granted to NRC employees and your associated reporting responsibilities; the proper handling and protection of sensitive unclassified and classified information; security-related policies and procedures associated with automated systems and the telecommunication of sensitive unclassified and classified information; and the need to coordinate certain meeting and travel arrangements with SEC.

Contact your Security Advisor for general security advice and assistance; your Authorized Classifier for classification guidance; or your Systems Security Officer for questions regarding automated systems. You may also want to refer to NRC Management Directive 2000 or call the Division of Security directly.

Because the threats and liabilities are quite real to you personally, and to the national security in general, compliance with NRC security policies and procedures is very important. One person can make a difference... and...YOU ARE THE KEY!

YOU ARE THE KEY TO NRC SECURITY

PERMISSIBLE ACCESS FOR NRC EMPLOYEES

(On a Need-To-Know Basis)

NRC employees may have access to the categories/levels of information listed below if they possess the security clearance ("Q" or "L") or the approval (145b) required as indicated; and if they have a demonstrated official need-to-know for the information.

Categories/Levels of Information at NRC	NRC Security Clearance/Approval		
	Q	L	145b
Sensitive Unclassified Information			
Official Use Only (OUO)	X	X	X
Proprietary	X	X	X
Safeguards (SGI)	X	X	X
Limited Official Use (LOU)	X	X	X
Classified Information			
National Security Information (NSI)			
Top Secret (TS)	X		
Secret (S)	X	X	
Confidential (C)	X	X	
Restricted Data (RD)			
Top Secret (TS)	X		
Secret (S)	X		
Confidential (C)	X	X*	

*For some C/RD relative to Naval Nuclear Propulsion Information, a "Q" is required.

ADP/WORD PROCESSING REMINDERS

In General:

- Do not process or telecommunicate classified information on automated systems, except under special circumstances and with the written approval of SEC.
- Protect access identifiers (e.g., passwords, logon procedures) to systems by holding them in confidence.
- Establish specific diskettes for classified and sensitive unclassified information. Mark and protect these diskettes according to the sensitivity of the information. Use the corresponding special diskette sleeves (red for classified; yellow for sensitive unclassified).
- Do not leave systems unattended during the processing of classified or sensitive unclassified information.
- Properly mark and protect or destroy printer ribbons and output containing classified and sensitive unclassified information according to its sensitivity.
- Assure information availability through appropriate back-up and storage (e.g., duplicating diskettes, archiving).
- Physically locate components (e.g., terminals, printers) to preclude unauthorized access/viewing. When not in use, store software inside a container (e.g., desk, file cabinet).

Specifically:

Shared Logic (5520)

- Use internal capabilities for limiting access to information by:
  1. establishing a profile, user I. D. and password with your Systems Security Officer;
  2. entering information in the format appropriate for the sensitivity of the information: shared revise, shared read, or private.

Personal Computers

- Do not store sensitive unclassified information on systems with non-removable disks unless approved in writing by SEC.
- If the system is left in an auto-answer mode, insure that no sensitive unclassified information is left in the machine or on the diskette(s).

Timesharing Computer Systems

- Do not disclose the telephone number of the host computer, its connect procedures, or your password.
- Notify your Account Coordinator when you no longer require access to the system or you suspect your password has been compromised.

Notes